

Claims

WHAT IS CLAIMED IS:

1. A method comprising:
attaching a secure router advertisement to an address update associated with
a mobile node; and
sending the address update including the attached secure router
advertisement to a correspondent node.
2. The method of claim 1 wherein the address update includes a Mobile
IPv6-compliant binding update.
3. The method of claim 1 wherein the address update is sent by a node
acting as a representative of the mobile node.
4. The method of claim 1 further comprising:
sending a secure router solicitation to one or more access routers; and
receiving the secure router advertisement, responsive to the secure router
solicitation.
5. The method of claim 1 further comprising:
sending a secure router solicitation to one or more access routers, the secure
router solicitation including an identifier of the mobile node; and
receiving the secure router advertisement responsive to the router
solicitation, the secure router advertisement including the identifier of the mobile
node.

1 6. The method of claim 1 wherein the mobile node is associated with a
2 home address and further comprising:

3 sending a secure router solicitation to one or more access routers, the secure
4 router solicitation including the home address of the mobile node; and

5 receiving the secure router advertisement responsive to the router
6 solicitation, the secure router advertisement including the home address of the
7 mobile node.

8 7. The method of claim 1 further comprising:

9 sending a router solicitation to one or more access routers, the secure router
10 solicitation including a public key associated with the mobile node; and

11 receiving the secure router advertisement responsive to the router
12 solicitation, the secure router advertisement including the public key.

13 8. The method of claim 1 wherein the secure router advertisement includes
14 a signature of an access router associated with an access network, wherein the
15 mobile node may receive one or more messages at an address that belongs to the
16 access network of the access router.

17 9. The method of claim 1 wherein the secure router advertisement includes
18 a signature of an access router associated with an access network, wherein a
19 representative of the mobile node may receive one or more messages at an address
20 that belongs to the access network of the access router.
21
22
23
24
25

1 10. The method of claim 1 wherein the mobile node is associated with a
2 cryptographically-generated address generated by a public key and the secure
3 router advertisement includes the same public key.

4 11. The method of claim 1 wherein the secure router advertisement includes
5 a nonce field populated with an identifier of the mobile node.

6 12. The method of claim 1 wherein the secure router advertisement includes
7 a nonce field populated with a home address of the mobile node.

8 13. The method of claim 1 wherein the secure router advertisement includes
9 a nonce field populated with a public key associated with the mobile node.

10 14. The method of claim 1 wherein the mobile node is associated with a
11 current address within an access network and the address update specifies the
12 current address of the mobile node.
13
14
15
16
17
18
19
20
21
22
23
24
25

1 15. A computer program product encoding a computer program for
2 executing on a computer system a computer process, the computer process
3 comprising:

4 attaching a secure router advertisement to an address update associated with
5 a mobile node; and

6 sending the address update including the attached secure router
7 advertisement to a correspondent node.

8
9 16. The computer program product of claim 15 wherein the address update
10 includes a Mobile IPv6-compliant binding update.

11 17. The computer program product of claim 15 wherein the address update
12 is sent by a node acting as a representative of the mobile node.

13
14 18. The computer program product of claim 15 wherein the computer
15 process further comprises:

16 sending a secure router solicitation to one or more access routers; and

17 receiving the secure router advertisement, responsive to the secure router
18 solicitation.

1 19. The computer program product of claim 15 wherein the computer
2 process further comprises:

3 sending a secure router solicitation to one or more access routers, the secure
4 router solicitation including an identifier of the mobile node; and

5 receiving the secure router advertisement responsive to the router
6 solicitation, the secure router advertisement including the identifier of the mobile
7 node.

8 20. The computer program product of claim 15 wherein the mobile node is
9 associated with a home address and the compute process further comprises:

10 sending a secure router solicitation to one or more access routers, the secure
11 router solicitation including the home address of the mobile node; and

12 receiving the secure router advertisement responsive to the router
13 solicitation, the secure router advertisement including the home address of the
14 mobile node.

15 21. The computer program product of claim 15 wherein the computer
16 process further comprises:

17 sending a router solicitation to one or more access routers, the secure router
18 solicitation including a public key associated with the mobile node; and

19 receiving the secure router advertisement responsive to the router
20 solicitation, the secure router advertisement including the public key.
21
22
23
24
25

1 22. The computer program product of claim 15 wherein the secure router
2 advertisement includes a signature of an access router associated with an access
3 network, wherein the mobile node may receive one or more messages at an
4 address that belongs to the access network of the access router.

5 23. The computer program product of claim 15 wherein the secure router
6 advertisement includes a signature of an access router associated with an access
7 network, wherein a representative of the mobile node may receive one or more
8 messages at an address that belongs to the access network of the access router.

9 24. The computer program product of claim 15 wherein the mobile node is
10 associated with a cryptographically-generated address generated by a public key
11 and the secure router advertisement includes the same public key.
12

13 25. The computer program product of claim 15 wherein the secure router
14 advertisement includes a nonce field populated with an identifier of the mobile
15 node.
16

17 26. The computer program product of claim 15 wherein the secure router
18 advertisement includes a nonce field populated with a home address of the mobile
19 node.

20 27. The computer program product of claim 15 wherein the secure router
21 advertisement includes a nonce field populated with a public key associated with
22 the mobile node.
23
24
25

1 28. The computer program product of claim 15 wherein the mobile node is
2 associated with a current address within an access network and the address update
3 specifies the current address of the mobile node.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 29. A system comprising:

2 a node that attaches a secure router advertisement to an address update
3 associated with a mobile node and sends the address update including the attached
4 secure router advertisement to a correspondent node.
5

6 30. The system of claim 29 wherein the address update includes a Mobile
7 IPv6-compliant binding update.

8 31. The system of claim 29 wherein the node is a representative of the
9 mobile node.
10

11 32. The system of claim 29 wherein the node is the mobile node.

12 33. The system of claim 29 wherein the node transmits a secure router
13 solicitation to one or more access routers.
14

15 34. The system of claim 29 wherein the secure router advertisement is
16 generated by an access router responsive to the receipt of a secure router
17 solicitation.

18 35. The system of claim 29 wherein the mobile node is associated with an
19 identifier and the mobile node transmits a secure router solicitation to one or more
20 access routers, the secure router solicitation including the identifier of the mobile
21 node.
22
23
24
25

1 36. The system of claim 29 wherein the mobile node is associated with an
2 identifier and the mobile node receives a secure router advertisement from an
3 access router, the secure router advertisement including the identifier of the mobile
4 node.

5 37. The system of claim 29 wherein the mobile node is associated with a
6 home address and the mobile node transmits a secure router solicitation to one or
7 more access routers, the secure router solicitation including the home address of
8 the mobile node.

9 38. The system of claim 29 wherein the mobile node is associated with a
10 home address and the mobile node receives a secure router advertisement from an
11 access router, the secure router advertisement including the home address of the
12 mobile node.

13 39. The system of claim 29 wherein the mobile node transmits a secure
14 router solicitation to one or more access routers, the secure router solicitation
15 including a public key of the mobile node.

16 40. The system of claim 29 wherein the mobile node receives a secure
17 router advertisement from an access router, the secure router advertisement
18 including a public key of the mobile node.

19 41. The system of claim 29 wherein the secure router advertisement
20 includes a signature of an access router associated with an access network,
21 wherein a mobile node is in the access network of the access router.
22
23
24
25

1 42. The system of claim 29 wherein the mobile node is associated with a
2 cryptographically-generated address generated by a public key and the secure
3 router advertisement includes the same public key.

4 43. The system of claim 29 wherein the secure router advertisement
5 includes a nonce field populated with an identifier of the mobile mode.
6

7 44. The system of claim 29 wherein the secure router advertisement
8 includes a nonce field populated with a home address of the mobile node.

9 45. The system of claim 29 wherein the secure router advertisement
10 includes a nonce field populated with a public key associated with the mobile
11 node.
12

13 46. The system of claim 29 wherein the mobile node is associated with a
14 current address within an access network and the address update specifies the
15 current address of the mobile node.
16
17
18
19
20
21
22
23
24
25

1 47. A method comprising:
2 receiving an address update from a mobile node, the address update
3 including a secure router advertisement, a purported identifier of the mobile node,
4 and a purported current address;
5 verifying that the secure router advertisement is signed by an authorized
6 access router;
7 verifying that the purported current address is associated with the
8 authorized access router; and
9 verifying the association between the purported identifier and the purported
10 current address using data from the secure router advertisement.
11

12 48. The method of claim 47 wherein the mobile node is a Mobile IPv6
13 mobile node.

14 49. The method of claim 47 wherein the address update is a Mobile IPv6
15 binding update.
16

17 50. The method of claim 47 wherein the purported identifier is a Mobile
18 IPv6 home address.

19 51. The method of claim 47 wherein the current address is a Mobile IPv6
20 care-of address.
21

22 52. The method of claim 47 wherein the operation of verifying the
23 association between the purported identifier and the purported current address
24 comprises:
25

 reading an identifier from the secure router advertisement; and

1 verifying that the purported identifier matches the identifier read from the
2 secure router advertisement.

3 53. The method of claim 47 wherein the operation of verifying the
4 association between the purported identifier and the purported current address
5 comprises:

6 reading a home address from the secure router advertisement; and
7 verifying that the purported identifier matches the home address.

8 54. The method of claim 47 wherein the purported identifier is a
9 cryptographically-generated address associated with the mobile node and the
10 operation of verifying the association between the purported identifier and the
11 current address comprises:

12 reading a public key from the secure router advertisement; and
13 verifying that the same public key was used to generate cryptographically-
14 generated address.
15

16 55. The method of claim 47 wherein the authorized access router is
17 associated with a subnet prefix specified in the secure router advertisement and the
18 operation of verifying that the purported current address is associated with the
19 authorized access router comprises:

20 verifying that the purported current address matches subnet prefix.
21
22
23
24
25

1 56. The method of claim 47 wherein the operation of verifying that the
2 secure router advertisement is signed by an authorized access router comprises:
3 verifying that a signature used to sign the secure router advertisement is
4 associated with an access router authorized by certification to advertise a subnet
5 , prefix specified in the secure router advertisement.
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 57. A computer program product encoding a computer program for
2 executing on a computer system a computer process, the computer process
3 comprising:

4 receiving an address update from a mobile node, the address update
5 including a secure router advertisement, a purported identifier of the mobile node,
6 and a purported current address;

7 verifying that the secure router advertisement is signed by an authorized
8 access router;

9 verifying that the purported current address is associated with the
10 authorized access router; and

11 verifying the association between the purported identifier and the purported
12 current address using data from the secure router advertisement.
13
14
15
16
17
18
19
20
21
22
23
24
25

1 58. The computer program product of claim 57 wherein the mobile node is
2 a Mobile IPv6 mobile node.

3 59. The computer program product of claim 57 wherein the address update
4 is a Mobile IPv6 binding update.

5 60. The computer program product of claim 57 wherein the purported
6 identifier is a Mobile IPv6 home address.

7 61. The computer program product of claim 57 wherein the current address
8 is a Mobile IPv6 care-of address.

9 62. The computer program product of claim 57 wherein the operation of
10 verifying the association between the purported identifier and the purported
11 current address comprises:

12 reading an identifier from the secure router advertisement; and
13 verifying that the purported identifier matches the identifier read from the
14 secure router advertisement.

15 63. The computer program product of claim 57 wherein the operation of
16 verifying the association between the purported identifier and the purported
17 current address comprises:

18 reading a home address from the secure router advertisement; and
19 verifying that the purported identifier matches the home address.

20 64. The computer program product of claim 57 wherein the purported
21 identifier is a cryptographically-generated address associated with the mobile node
22
23
24
25

1 and the operation of verifying the association between the purported identifier and
2 the current address comprises:

3 reading a public key from the secure router advertisement; and
4 verifying that the same public key was used to generate the
5 cryptographically-generated address.

6 65. The computer program product of claim 57 wherein the authorized
7 access router is associated with a subnet prefix specified in the secure router
8 advertisement and the operation of verifying that the purported current address is
9 associated with the authorized access router comprises:

10 verifying that the purported current address matches the subnet prefix.

11
12 66. The computer program product of claim 57 wherein the operation of
13 verifying that the secure router advertisement is signed by an authorized access
14 router comprises:

15 verifying that a signature used to sign the secure router advertisement is
16 associated with an access router authorized by certification to advertise a subnet
17 prefix specified in the secure router advertisement.

1 67. A system comprising:

2 a correspondent node that receives an address update from a mobile node,
3 the address update including a secure router advertisement, a purported identifier
4 of the mobile node, and a purported current address, the correspondent node
5 verifying that the secure router advertisement is signed by an authorized access
6 router, that the purported current address is associated with the authorized access
7 router, and that data from the secure router advertisement associates the purported
8 identifier with the purported current address.

9
10 68. The system of claim 67 wherein the mobile node is a Mobile IPv6
11 mobile node.

12 69. The system of claim 67 wherein the address update is a Mobile IPv6
13 binding update.

14
15 70. The system of claim 67 wherein the purported identifier is a Mobile
16 IPv6 home address.

17 71. The system of claim 67 wherein the current address is a Mobile IPv6
18 care-of address.

19
20 72. The system of claim 67 wherein the correspondent nodes matches the
21 purported identifier to an identifier read from the secure router advertisement.

22 73. The system of claim 67 wherein the correspondent nodes matches the
23 purported identifier to a home address read from the secure router advertisement.
24
25

1 74. The system of claim 67 wherein the purported identifier is a
2 cryptographically-generated address, the secure router advertisement includes a
3 public key, and the correspondent verifies that the same public key was used to
4 generate the cryptographically-generated address.

5 75. The system of claim 67 wherein the authorized access router is
6 associated with a subnet prefix specified in the secure router advertisement and the
7 correspondent node verifies that the purported current address matches the subnet
8 prefix.

9 76. The system of claim 67 wherein the correspondent node verifies that a
10 signature used to sign the secure router advertisement is associated with an access
11 router authorized by certification to advertise a subnet prefix specified in the
12 secure router advertisement.
13
14
15
16
17
18
19
20
21
22
23
24
25

1 77. One or more computer-readable media storing a data structure
2 comprising:

3 a first data field storing a home address of a soliciting mobile node; and
4 a second data field storing a subnet prefix specifying an access network in
5 which the mobile node is located.

6
7 78. The computer-readable media of claim 77 wherein the data structure
8 further comprises:

9 a signature of an access router authorized to advertise the subnet prefix of
10 the access network.

1 79. One or more computer-readable media storing a data structure
2 comprising:

3 a first data field storing a public key of a soliciting mobile node; and
4 a second data field storing a subnet prefix specifying an access network in
5 which the mobile node is located.

6
7 80. The computer-readable media of claim 79 wherein the data structure
8 further comprises:

9 a signature of an access router authorized to advertise the subnet prefix of
10 the access network.

1 81. One or more computer-readable media storing a data structure
2 comprising:

3 a first data field storing a purported identifier of a mobile node;

4 a second data field storing a current address at which the mobile node is
5 purported located; and

6 a third data field storing a secure router advertisement signed by an access
7 router authorized to advertise the subnet prefix of the access network that includes
8 the purported current address.

9
10 82. The computer-readable media of claim 81 wherein the purported
11 identifier is a Mobile IPv6 home address.

12 83. The computer-readable media of claim 81 wherein the purported current
13 address is a Mobile IPv6 care-of address.

14 84. The computer-readable media of claim 81 wherein the purported
15 identifier is a public key.

16
17 85. The computer-readable media of claim 81 wherein the secure router
18 advertisement includes the purported identifier in the nonce field.

1 86. A computer program product encoding a computer program for
2 executing on a computer system a computer process, the computer process
3 comprising:

4 generating a secure router advertisement data structure, wherein a nonce
5 field of the a secure router advertisement data structure contains a member of a set
6 containing an IPv6 address, a home address, an identifier, a group identifier, a
7 cryptographic identifier, and a public key.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25